MERENKULUN KYBERTURVALLISUUS – ALUSTEN PARHAAT KÄYTÄNNÖT

HUOLTOVARMUUSORGANISAATIO
VESIKULJETUSPOOLI

www.huoltovarmuus.fi

Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa.

Huoltovarmuuskeskus (HVK) on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen liittyvä suunnittelu ja operatiivinen toiminta.

Huoltovarmuuskeskuksen yhteydessä toimii Huoltovarmuusneuvosto sekä pysyvinä yhteistyöeliminä komitean tapaan toimivia sektoreita ja pooleja. Nämä yhdessä muodostavat Huoltovarmuusorganisaation.

HUOLTOVARMUUSORGANISAATIO
VESIKULJETUSPOOLI

Julkaisija:	Huoltovarmuusorganisaatio, Vesikuljetuspooli
Teksti:	Teksti perustuu Huoltovarmuusorganisaatioon kuuluvan Vesikuljetuspoolin ja Suomen Varustamot ry:n tilaamaan ja Deductive Labs Ab:n toteuttamaan selvitykseen
Kuvat:	Shutterstock
Taitto:	Up-to-Point Oy
Julkaisu-vuosi:	2021
ISBN:	978-952-5608-96-0

Sisältö

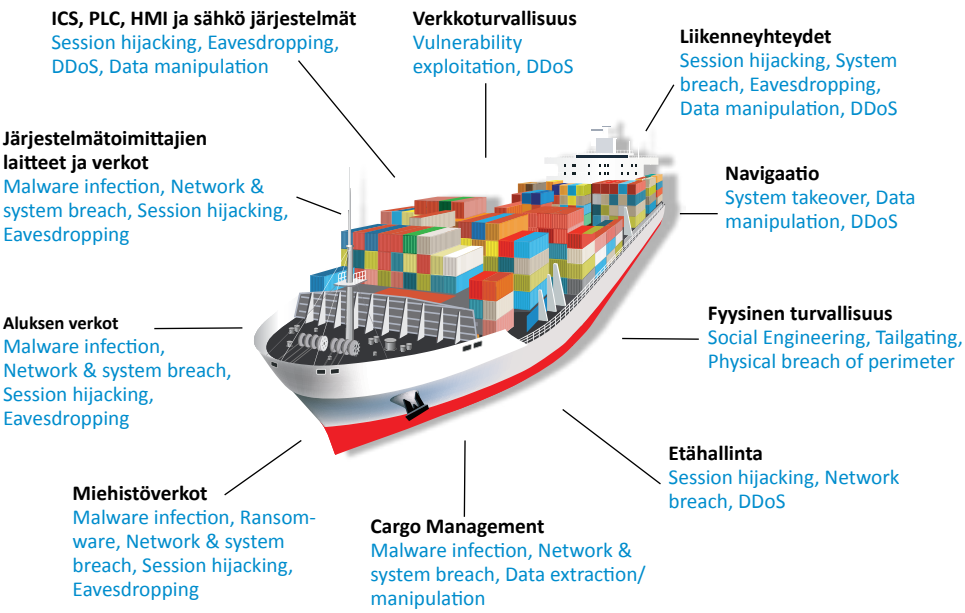
Aluksen kyberturvallisuuden eri osa-alueita ja parhaita käytäntöjä ehdotetaan ja esitetään tässä asiakirjassa seuraavasti:

TAUSTA JA ESITTELY

Merenkulkuala ja kauppa-alukset voivat tuntua epätodennäköisiltä kohteilta kyberhyökkäyksille, mutta merenkulkualan digitalisoitumisen lisääntyessä ja verkkoon liitetyn tietotekniikan (IT), operatiivisen tekniikan lisääntyessä (OT) -järjestelmät, meriteollisuuden ohjausjärjestelmät (ICS) ja mm satelliittiviestintä ovat alttiita verkkorikollisten ja muiden tietoturvallisuutta uhkaavien ryhmien hyökkäyksille. Siksi on kriittistä, että kyberturvallisuutta hallitaan asianmukaisesti merenkulkualalla alusten, miehistön ja rahdin suojaamiseksi mahdollisilta kyberturvallisuusuhkilta ja -hyökkäyksiltä.

Merenkulun kyberturvallisuus on käytäntöjen, menettelyjen, ohjeiden, toimenpiteiden, riskienhallintatoimien, koulutuksien, työkalujen ja tekniikoiden valintoja, joita käytetään koko merenkulkualan ja alusten suojaamiseen.

IT- ja OT-järjestelmiin liittyvät riskit ovat erilaiset siinä mielessä, että IT-järjestelmien riskit vaikuttavat pääasiassa talouteen ja maineeseen, kun taas OT-järjestelmien riskit voivat vaikuttaa turvallisuuteen ja uhata ihmishenkiä, omaisuutta ja ympäristöä, jos riskit toteutuvat.



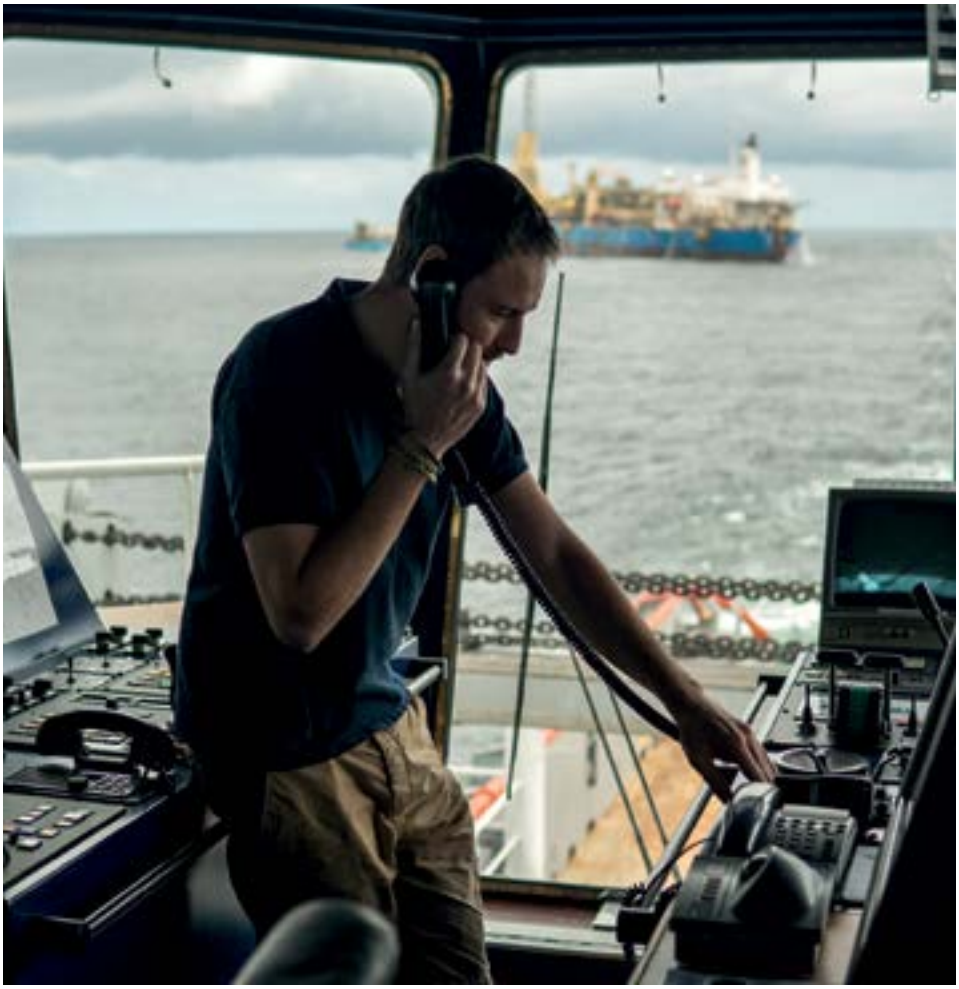
Tammikuussa 2021 Suomen Varustamot ry yhdessä Huoltovarmuuskeskuksen kanssa aloitti hankkeen merenkulkualan aluksien kyberturvallisuuden tilanteen kartoittamiseksi. Suomalainen merenkulun kyberturvallisuusasiantuntija Deductive Labs Ab valittiin toteuttamaan projektin.

Hankkeessa tuotettiin kolme erillistä asiakirjaa, jotka ovat saatavissa kieliversioineen (en, fi, sv) Suomen Varustamot r.y:n tai Huoltovarmuuskeskuksen julkaisu-sivujen kautta: *https://www.huoltovarmuuskeskus.fi/julkaisut* ja *https://shipowners.fi/vastuullisuus/turvallisuus/kyberturvallisuus/*

1. ***Merenkulun kyberturvallisuusraportti – Suomen kauppalaivaston kypsyys (ENG)***, kattava raportti Suomen merenkulkualan nykytilasta

2. ***Merenkulun kyberturvallisuus – Alusten parhaat käytännöt***, yhteenveto havainnoista ja esitys alusten parhaista käytännöistä

3. ***Merenkulun kyberturvallisuus – Varustamon parhaat käytännöt***, yhteenveto havainnoista ja esitys varustamojen parhaista käytännöistä



1. ALUSTEN KRIITTISTEN PALVELUJEN JA TOIMINTOJEN RISKIT

- Tunnista kaikki alusten kriittiset palvelut ja toiminnot (navigaatio, käyttövoima, vakaus, painolasti, jne.)
- Tunnista kaikki kriittisten palvelujen ja toimintojen IT- ja OT-järjestelmät (tietokoneet, verkot, ohjaus- ja automaatiojärjestelmät, siltajärjestelmät, navigointi, työntövoima ja koneet jne jne.)
- Tunnista riskit ja niiden vaikutukset kaikkiin kriittisiin palveluihin, toimintoihin ja järjestelmiin
- Luo riskinhallintasuunnitelma tunnistettujen riskien korjaamiseksi ja minimoimiseksi
- Päivitä omaisuusluettelo ja riskinarviointi aina kun muutoksia tapahtuu

Vinkkejä:

Käytä vakiintuneiden ISM / ISPS-menettelyjen riskienhallintamenetelmiä, jos sellaisia on sovellettavissa ja käytettävissä. Jos vakiintuneita riskienhallinta malleja ei ole käytettävissä, käytä esim. DCSA(Digital Container Ship Association):n julkaistamia malleja:

- DCSA Asset List Risk Assessment Framework examples
- DCSA Asset Management and Risk Register Templates Reading Guide

Tavoite:

- Alusten kriittiset palvelut, toiminnot ja näihin käytetyt IT- ja OT-järjestelmät on dokumentoitu ja riskit tunnistettu
- Alukset noudattavat IMO MSC.428(98) vaatimuksia merenkulun kyberturvallisuusriskien hallinnasta
- Riskinhallintasuunnitelma kuvaa toimenpiteet joilla korjataan tunnistetut riskit

Vastuuhenkilöt:

- Aluksen IT- ja OT-järjestelmistä vastaavat avainhenkilöt
- Organisaation IT- ja Kyberturvallisuudesta vastaavat henkilöt

Huomioon otettavat asiat:

- ❑ *Laivaverkot ja tietokoneet*
- ❑ *Komentosiltajärjestelmät*
- ❑ *Lastinkäsittely- ja hallintajärjestelmät*
- ❑ *Propulsio-, kone- ja tehonsäätöjärjestelmät*
- ❑ *Kulunvalvontajärjestelmät*
- ❑ *Matkustajiin liittyvät hallinnolliset järjestelmät*
- ❑ *Matkustajat, jotka käyttävät julkisia verkkoja*
- ❑ *Varustamon hallinnolliset järjestelmät*
- ❑ *Miehistöön liittyvät hallinnolliset järjestelmät*
- ❑ *Viestintäjärjestelmät*

2. VERKKOJEN SEGMENTOINTI

Aluksilla käytettävät kriittiset palvelut, funktiot ja järjestelmät olisi segmentoitava eri verkkoihin niiden suojelemiseksi ja mahdollisten hyökkäysten rajoittamiseksi. Verkkosegmentointi on kriittisissä verkoissa käytetty vakio periaate ja yksi standardien, kuten ISO27001 ja ISA / IEC62443, keskeisistä vaatimuksista.

1. Tunnista kaikki kriittiset järjestelmät ja arvioi nykyinen verkon suunnittelu ja segmentointi
2. Luo verkot kriittisten järjestelmien eri ryhmille, kuten viestintä-, silta-, koneisto-, rahti-, hallinto-, liike-, miehistö- ja wi-fi-verkot
3. Siirrä järjestelmät segmentoituihin verkkoihin ja päivitä palomuurisäännöt ja käytännöt vastaavasti (vaihe 3)

Vinkkejä:

Käytä standardeja, kuten ISO27001 tai ISA/IEC 62443, saadaksesi lisätietoja segmentoinnista ja eri suojavyöhykkeiden käyttämisestä kyberturvallisuuden sietokyvyn parantamiseksi kriittisissä järjestelmissä. Luo verkkokaaviot aluksille, jotta verkot ja järjestelmät voidaan helposti visualisoida. Aloita segmentoimalla ”helpoin” verkko, kuten miehistöverkot ja vierasverkot, ennen kuin aloitat kriittisten verkkojen ja järjestelmien segmentoinnin. Yhdistä samanlaiset järjestelmät ja resurssit samaan verkkoon järjestelmän toimivuuden ja kriittisyyden perusteella, mutta varmista, että vältät liikaa segmentointia, joka on haitallista toiminnalle.

Tulokset:

- Kriittiset IT- ja OT-järjestelmät (silta, moottori,jne.) on segmentoitu eri verkkoihin

Vastuuhenkilöt:

- Aluksen IT- ja OT-järjestelmistä vastaavat avainhenkilöt
- Organisaation IT-, verkko ja Kyberturvallisuudesta vastaavat henkilöt

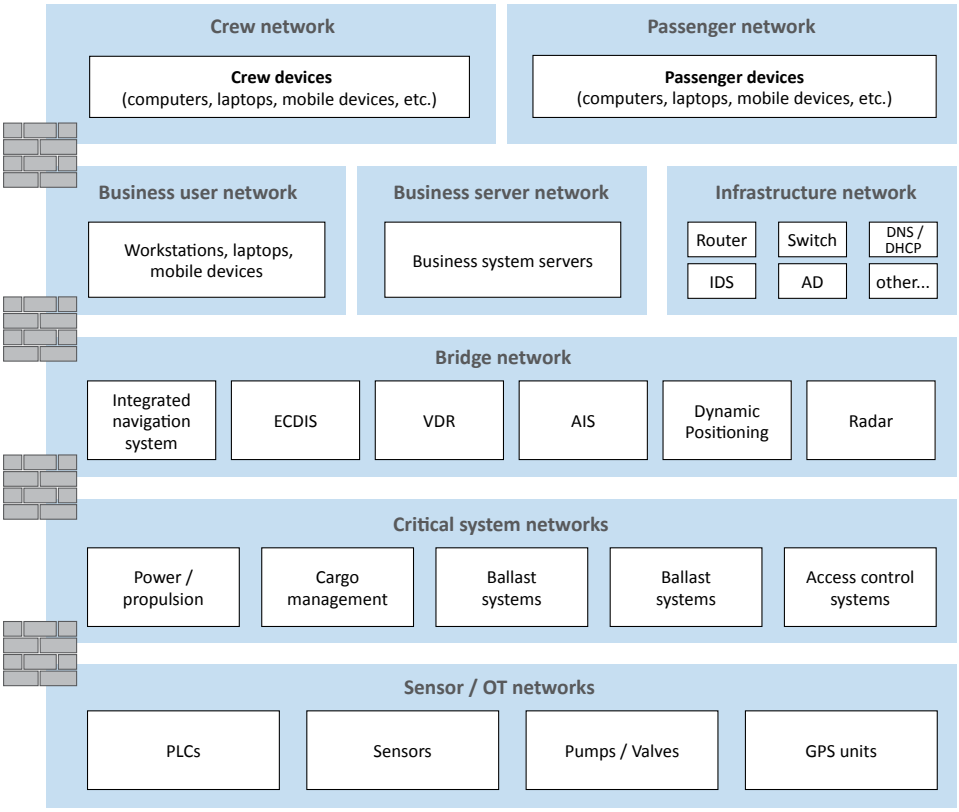
Huomioon otettavat asiat:

Verkon segmentointi alusten verkkojen:

- ❑ *Hallinnolliset verkot*
- ❑ *Miehistöverkot*
- ❑ *Wifi-verkot*
- ❑ *Matkustajaverkot*
- ❑ *Pääkoneisto-, sähkövoima-, ja muut koneistoverkot*
- ❑ *Toimittajaverkot*
- ❑ *Muut verkot*

tarpeen mukaan riskianalyysin avulla

Esimerkki verkkokaavio aluksen verkkojen segmentoinnista:



3. PALOMUURIEN MÄÄRITTÄMINEN

Kun järjestelmät on segmentoitu, on tärkeää, että verkkoihin ja järjestelmiin sovelletaan asianmukaisia palomuuri käytäntöjä, jotka sallivat vain hyväksytyn ja tarvittavan liikenteen aluksen järjestelmiin.

1. Varmista, että kaikki järjestelmät ja verkot ovat asianmukaisesti suojattuja. Salli vain tarvittavat käyttöoikeudet ja vältä pääsyä julkisista, hyväksymättömistä lähteistä. Kiinnitä erityistä huomiota alusten viestintäjärjestelmiin (VSAT, varustamon ja aluksen laajakaista, jne.) Suojaa järjestelmät suodattamalla liikenne, segmentoimalla järjestelmät ja soveltamalla turvallisia konfiguraatioita (katso vaihe 8 – Järjestelmien tietoturvakonfigurointi)
2. Tunnista järjestelmien asianmukaiseen käyttöön tarvittavat IP-osoitteet, verkkoyhteydet ja tietovirrat
3. Analysoi palomuurikäytännöt ja varmista, että vain tarvittava tiedonsiirto on sallittu
4. Määritä palomuurit oletusarvoisesti estämään ja kirjaamaan kaikki ei hyväksytty liikenne (default-deny policy)

Vinkkejä:

Käytä tunnistettuja järjestelmä- ja resurssiryhmiä sekä verkko- ja tiedonsiirtokaavioita (data-flow diagram), jotka on luotu verkon segmentoinnin aikana (vaihe 2) ja varmista, että järjestelmille ja verkoille luodaan asianmukaiset palomuurikäytännöt järjestelmien tiedonsiirtovaatimuksien perusteelta.

Tulokset:

- Palomuurikäytännöt on määritelty ja sallivat ainoastaan järjestelmien toimivuuteen tarvittavan liikenteen

Vastuuhenkilöt:

- Aluksen IT- ja OT-järjestelmistä vastaavat avainhenkilöt
- Organisaation IT-, verkko ja Kyberturvallisuudesta vastaavat henkilöt

Huomioon otettavat asiat:

- ❑ *Aluksen palomuurit*
- ❑ *Segmentoidut verkot ja järjestelmät sekä suojattava tieto*

4. KRIITTISTEN VERKKOJEN JA JÄRJESTELMIEN ETÄYHTEYDET

Useimmat alukset käyttävät kolmansia osapuolia ja toimittajia alusten kriittisten järjestelmien hallintaan ja seurantaan. On tärkeää valvoa kriittisten järjestelmien etäkäyttöä ja paikallista pääsyä ulkopuolisille toimittajille ja sisäisille käyttäjille.

1. Tunnista kolmannet osapuolet ja sisäiset käyttäjät, jotka tarvitsevat pääsyn aluksen verkkoihin ja järjestelmiin.
2. Tunnista ja dokumentoi IP-osoitteet, verkkoportit / -palvelut ja -resurssit, joita he tarvitsevat
3. Päivitä palomuurikäytännöt, jotta kolmannet osapuolet ja käyttäjät voivat turvallisesti käyttää niitä verkkoja, järjestelmiä ja palveluja joita he tarvitsevat
4. Dokumentoi kaikki etäyhteydet ja varmista, että asianmukaiset etätyö käytännöt ovat dokumentoituja.
5. Hallitse toimittajien paikallista pääsyä aluksen kriittisiin järjestelmiin ja verkkoihin. Varmista, että toimittajat eivät kytke suojaamattomia laitteita aluksen verkkoihin, ja valvo tarvittaessa käyttöä.

Vinkkejä:

Käytä kolmansien osapuolten ja toimittajien dokumentaatioita tunnistaaksesi järjestelmän käyttövaatimukset, joita voidaan käyttää palomuurikäytännöissä. Luo määräyksiä jotka kuvaavat organisaation vaatimukset etäyhteyksille (VPN yhteydet, henkilökohtaiset käyttäjät, vahvat salasanat / MFA, haittaohjelmien torjunta, jne.).

Tulokset:

- Alusten kriittisten verkkojen ja järjestelmien etäkäyttö on hallittua
- Etäkäyttöä koskevat vaatimukset ja sopimukset on tehty kolmansien osapuolien ja toimittajien kanssa

Vastuuhenkilöt:

- Aluksen IT- ja OT-järjestelmistä vastaavat avainhenkilöt
- Organisaation IT-, verkko ja Kyberturvallisuudesta vastaavat henkilöt
- Ulkoiset järjestelmätoimittajat ja kolmannet osapuolet

Huomioon otettavat asiat:

- ❑ *Luettelo kolmansista osapuolista ja järjestelmätoimittajista*
- ❑ *Kriittiset järjestelmät, joita kolmannet osapuolet ja toimittajat*
- ❑ *Etäyhteyksien toiminnan ohjeita toimittajalle hallinnoivat*

5. HAITTAOHJELMIEN TORJUNTA

Haittaohjelmien torjunta on kyberturvallisuuden peruskomponentti ja on suositeltavaa että alusten kriittisiin järjestelmiin asennetaan haittaohjelmien torjuntaohjelmisto. EDR-ratkaisuja (end-point-protection-and-response) suositellaan, koska ne suojaavat sekä järjestelmiä että tarjoavat edistyneitä seuranta- ja reagointimahdollisuuksia haittaohjelmatartuntojen sattuessa.

1. Asenna ja määritä haittaohjelmien torjuntaohjelmisto kaikkiin kriittisiin järjestelmiin mahdollisuuksien mukaan (Windows, Linux, MacOS)
2. Varmista, että haittaohjelmien torjuntaohjelmisto päivitetään säännöllisesti ja automaattisesti.
3. Tunnista järjestelmät, joihin haittaohjelmien torjuntaa ei voida asentaa, ja luo ohjauksia näille järjestelmille (verkon segmentointi, tiukka käyttöoikeus) jne.). Esimerkiksi ECDIS-järjestelmät ovat tyypillisesti tyyppihyväksyttyjä ja tapauskohtaisia asennuksia ei sallita ja tarvitaan erilaisia suojaustoimenpiteitä.
4. Varmista, että kaikki ulkoiset USB- laitteet ja vastaavat laitteet tarkistetaan haittaohjelmien varalta ennen käyttöä aluksen kriittisissä järjestelmissä.

Vihjeitä:

Varmista, että kaikissa järjestelmissä on haittaohjelmien torjuntaohjelmisto asennettu suojaamaan haittaohjelmilta. Ohjelmisto suojaa järjestelmiä haittaohjelmilta eri lähteistä kuten sähköposti, verkkosivustot ja USB-asemat ja muut lähteet ja järjestelmät joita käytetään aluksilla.

Tavoite:

- Haittaohjelmien torjuntaohjelmisto on otettu käyttöön kaikissa aluksen järjestelmissä mahdollisuuksien mukaan.
- Järjestelmät, joihin ei voida asentaa haittaohjelmien torjuntaa, on tunnistettu, ja vaihtoehtoiset menetelmät on tunnistettu ja toteutettu näiden järjestelmien suojaamiseksi haittaohjelmilta

Vastuuhenkilöt:

- Aluksen IT- ja OT-järjestelmistä vastaavat avainhenkilöt
- Organisaation IT-, verkko ja Kyberturvallisuudesta vastaavat henkilöt

Huomioon otettavat asiat:

- ❑ *Varmista, että haittaohjelmien suojausjärjestelmät päivitetään säännöllisesti*
- ❑ *Varmista, että haittaohjelmien suojausjärjestelmän tapahtumat kirjataan, analysoidaan ja poikkeamiin reagoidaan asianmukaisesti*

6. JÄRJESTELMIEN MONITOROINTI JA LOKITUS

Järjestelmien monitorointi ja tapahtumien lokitus ovat välttämättömiä tehokkaan kyberhyökkäyksien valvonnan mahdollistamiseksi. Ilman asianmukaista monitorointia ja tapahtumien lokitusta on erittäin vaikea havaita hyökkäyksiä ja reagoida niihin.

1. Ota käyttöön monitorointi- ja lokienhallintajärjestelmä alusten IT- ja OT-järjestelmien tapahtumien seurantaan
2. Määritä kaikki aluksen IT- ja OT-järjestelmät lähettämään tapahtumatietoja keskitettyyn lokienhallintajärjestelmään
3. Määritä kaikki aluksen palomuurit ja verkkolaitteet lähettämään tapahtumatietoja keskitettyyn lokienhallintajärjestelmään
4. Analysoi lokeja jatkuvasti hyökkäysten havaitsemiseksi

Vihjeitä:

Markkinoilla on monia lokienhallintajärjestelmiä, joita voidaan käyttää. Loki- ja analyysipalvelut voidaan ulkoistaa luotetulle kumppanille, jolla on tietoa ja kykyä toimittaa lokianalyysi palveluja.

Tulokset:

- Alusten kriittisiä järjestelmiä seurataan ja lokien tuottamat poikkeamatiedot lähetetään keskitettyyn ratkaisuun analysointia varten

Vastuuhenkilöt:

- Aluksen IT- ja OT-järjestelmistä vastaavat avainhenkilöt
- Organisaation IT-, verkko ja Kyberturvallisuudesta vastaavat henkilöt

Huomioon otettavat asiat:

- ❑ *Kaikki aluksen IT- järjestelmät*
- ❑ *OT-järjestelmät joilla on mahdollisuus tuottaa lokitietoja*

7. JÄRJESTELMIEN SÄÄNNÖLLINEN PÄIVITYS

Hyökkääjien yleisin tapa hyödyntää haavoittuvuuksia on hyökätä haavoittuviin järjestelmiin ja sovelluksiin. Siksi on tärkeää päivittää järjestelmät ja sovellukset säännöllisesti järjestelmien suojaamiseksi, jotta mahdolliset hyökkääjät eivät voi hyödyntää haavoittuvuuksia.

1. Seuraa toimittajien ja viranomaisten julkaisemia haavoittuvuus tiedotteita
2. Päivitä kriittiset järjestelmät ja sovellukset säännöllisesti korjaamaan haavoittuvuudet
3. Kiinnitä erityistä huomiota järjestelmiin ja sovelluksiin, jotka ovat yhteydessä epäluotettaviin verkkohin tai Internettiin. Varmista, että näitä järjestelmiä päivitetään säännöllisesti
4. Määrittele päivitysmenettelyiden ja korjaustoimenpiteiden vastuut ja varmista että järjestelmiä päivitetään säännöllisesti ja hallitusti kun on mahdollista (telakalla, satamassa, merellä jne.)

On suositeltavaa toteuttaa vähintään kuukausittaiset säännölliset päivitykset, mutta on myös varmistettava, että IT-ryhmät pystyvät tarvittaessa asentamaan kriittiset päivitystiedot nopeasti.

Vinkkejä:

Järjestelmien ja sovellusten korjaaminen voi olla vaikeaa ja aikaa vievää, varsinkin jos työ on tehtävä manuaalisesti. Suosittelemme erilaisten automatisointityökalujen käyttöönottoa helpottamaan päivityksien ja korjaustoimenpiteiden asennusta. Automaatio vähentää manuaalista työpanosta ja siten tarvittavia henkilöresursseja ja varmistaa standardoidun menetelmän päivityksen ja korjaustoimenpiteiden asennukseen.

Tulokset:

- Aluksissa käytettävät järjestelmät ja sovellukset on päivitetty

Vastuullinen:

- Aluksen IT- ja OT-järjestelmistä vastaavat avainhenkilöt
- Organisaation IT-, verkko ja Kyberturvallisuudesta vastaavat henkilöt
- Ulkoiset järjestelmätoimittajat ja kolmannet osapuolet

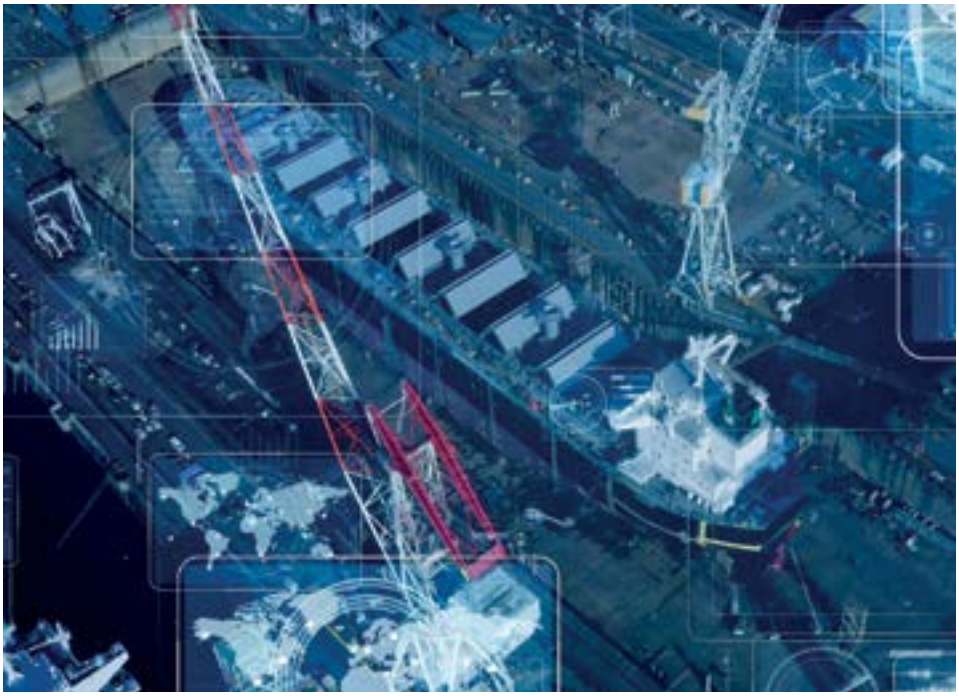
Huomioon otettavat asiat:

- ❑ *Korjaustoimenpiteet järjestelmän kriittisyyden mukaan*
- ❑ *Viestintä korjaustoimenpiteistä järjestelmästä vastaavien henkilöiden kanssa (sisäinen, ulkoinen toimittaja, jne.)*

8. JÄRJESTELMIEN TIETOTURVAKONFIGUROINTI

Järjestelmän kovennus on prosessi, jolla varmistetaan, että kaikki järjestelmät ja sovellukset on konfiguroitu oikein ja turvallisesti parhaiden käytäntöjen mukaisesti. Tähän sisältyy järjestelmänvalvojien salasanojen, kokoonpanojen, käytettyjen verkkoprotokollien (telnet vs ssh), verkon segmentointi jne..

1. Päivitä kaikkien järjestelmien oletussalasanat (Satcom, Navigointi, koneiston ohjausjärjestelmät, Sarja-IP-muuntimet jne.)
2. Varmista, että kaikki sisäiset Wi-Fi-verkot on suojattu oikein ja määritetty vahvoilla salasanoilla ja protokollilla.
3. Suojatut USB-portit. Varmista että vain hyväksyttyjä, tarkastettuja ja suojattuja USB-laitteita käytetään. Tarkista, ettei USB-laitteissa ole haittaohjelmia, ennen kuin kytket ne kriittisiin järjestelmiin.
4. Älä kytke henkilökohtaisia, suojaamattomia laitteita alualuksen verkkoihin tai järjestelmiin. Käytä vain nimettyjä miehistön verkkoja.
5. Luo vakiokonfiguraatiot kaikille järjestelmille ja sovelluksille, joissa kyberturvallisuus otetaan huomioon.
6. Ota standardoidut kokoonpanot käyttöön järjestelmissä ja sovelluksissa.
7. Luo tarkistuslistoja uusien järjestelmien käyttöönottoon (vaihda oletussalasanat, määritä suojatut asetukset, jne.)



Vinkkejä:

Käytä valmiita työkaluja järjestelmien konfigurointiin ja standardoitujen prosessien luomiseen. Automaattisilla päivitystyökaluilla ja prosessien käytöllä varmistetaan että esimerkiksi oletussalasanat vaihdetaan ja että käytetään turvallisia määrityksiä ja protokollia.

Kiinnitä erityistä huomiota aluksen kriittisiin järjestelmiin, kuten ECDIS, integroidut siltajärjestelmät, tutka, GPS jne., jotka toteuttavat alukselle kriittisiä toimintoja ja varmista että on olemassa asianmukaiset menettelyt näiden järjestelmien suojaamiseksi hyökkäyksiltä ja häirinnältä.

Tulokset:

- Turvalliset vakiomääritykset ja kokoonpanot ovat dokumentoituja ja näitä voidaan käyttää kaikissa varustamon aluksien järjestelmissä ja sovelluksissa.
- Vakiomääritykset on otettu käyttöön alusten järjestelmissä ja sovelluksissa keskitetysti

Vastuullinen:

- Aluksen IT- ja OT-järjestelmistä vastaavat avainhenkilöt
- Organisaation IT-, verkko ja Kyberturvallisuudesta vastaavat henkilöt
- Ulkoiset järjestelmätoimittajat ja kolmannet osapuolet

Huomioon otettavat asiat:

- ❑ *Toimittajajärjestelmien automatisointi voi olla vaikeaa tai mahdotonta.*
- ❑ *Varmista, että toimittajat noudattavat yrityksen järjestelmiin asettamia vaatimuksia ja menettelyjä.*

9. TOIMITTAJIEN KYBERTURVALLISUUS

Useimmissa aluksissa käytetään kolmansia osapuolia ja toimittajia alusten kriittisten järjestelmien ja hallintaan ja valvontaan. On tärkeää tietää mitä kolmansia osapuolia ja toimittajia käytetään, ja varmistetaan että heillä on asianmukaiset kyberturvallisuuden valvontatoimet. Sopimusten tulisi sisältää organisaation kyberturvallisuusvaatimukset ja -vastuut, joita heidän on noudatettava palvelunsa toimittamisessa.

1. Määrittele kyberturvallisuusvaatimukset kolmansille osapuolille ja toimittajille, jotka varmistavat, että niiden toimitus on turvallista.
2. Vaadi että kolmansien osapuolien ja toimittajien käyttämät järjestelmät ja palvelut ovat turvallisia
3. Varmista, että ulkopuolisia osapuolia ja toimittajia valvotaan kriittisten järjestelmien kanssa työskenneltäessä

Vinkkejä:

Kyberturvallisuuden sanotaan yleensä olevan yhtä turvallinen kuin heikoin lenkki. Toimittajien kyberturvallisuus on siksi tärkeää ja sitä on hallittava, jotta kyberturvallisuutta hallitaan asianmukaisesti. Varmista, että kyberturvallisuusvaatimukset ja -vastuut dokumentoidaan ja sovitaan toimittajan kanssa.

Tulokset:

- Toimittajasopimukset sisältävät vaatimukset, jotka määrittelee toimittajan kyberturvallisuuden tason

Vastuussa:

- Organisaation IT-, verkko ja Kyberturvallisuudesta vastaavat henkilöt
- Marine operations
- Ulkoiset järjestelmätoimittajat ja kolmannet osapuolet

Huomioon otettavat asiat:

❑ *Kaikki kolmannet osapuolet ja toimittajat ja näiden kyberturvallisuus*

10. KYBERTURVALLISUUSKOULUTUS

Kyberturvallisuus koulutus ja tietoisuus ovat tärkeitä koko organisaatiolle ylimmästä johdosta työntekijöihin ja miehistöön. Saadakseen perustiedot kyberturvallisuudesta ja siitä, miten se vaikuttaa alukseen, henkilöstön tulee saada kyberturvallisuuskoulutusta. Tämä varmistaa, että aluksen henkilöstöllä on tieto ja ymmärrys siitä, mitä kyberturvallisuus on ja miten heidän tulisi toimia aluksen suojaamiseksi.

1. Järjestä kyberturvallisuuskoulutusta henkilöstölle
2. Tarjoa räätälöityä ja asiaankuuluvaa koulutusta henkilöstön eri rooleille
3. Toimeenpane kyberturvallisuus koulutus säännöllisesti
4. Järjestä kyberturvallisuuskoulutusta jatkuvana osana yrityksen prosesseja ja kulttuuria

Vinkkejä:

Käytä ulkopuolisia kouluttajia ja verkkokoulutusta säännöllisen kyberturvallisuuskoulutuksen tarjoamiseksi henkilöstölle.

Tulokset:

- Parempi ymmärrys kyberturvallisuudesta kaikille työntekijöille
- IMO: n kyberriskien hallintaa koskevien ohjeiden mukainen

Vastuussa:

- Organisaation kyberturvallisuudesta vastaavat henkilöt
- Alusten päälliköt

Huomioon otettavat asiat:

- ❑ *Tarjoa koulutusta kaikille työntekijöille, myös ylimmälle johdolle.*
- ❑ *Räätälöity ja asiaankuuluva koulutus eri rooleille*

HUOLTOVARMUUSORGANISAATIO
VESIKULJETUSPOOLI